

12. PRESENTATIONS AND GROUPS OF SMALL ORDER

Definition-Lemma 12.1. *Let A be a set. A **word** in A is a string of elements of A and their inverses. We say that the word w' is obtained from w by a **reduction**, if we can get from w to w' by repeatedly applying the following rule,*

- *replace aa^{-1} (or $a^{-1}a$) by the empty string.*

*Given any word w , the **reduced word** w' associated to w is any word obtained from w by reduction, such that w' cannot be reduced any further.*

*Given two words w_1 and w_2 of A , the **concatenation** of w_1 and w_2 is the word $w = w_1w_2$. The empty word is denoted e .*

*The set of all reduced words is denoted F_A . With product defined as the reduced concatenation, this set becomes a group, called the **free group with generators A** .*

It is interesting to look at examples. Suppose that A contains one element a . An element of $F_A = F_a$ is a reduced word, using only a and a^{-1} . The word $w = aaaa^{-1}a^{-1}aaa$ is a string using a and a^{-1} . Given any such word, we pass to the reduction w' of w . This means cancelling as much as we can, and replacing strings of a 's by the corresponding power. Thus

$$\begin{aligned} w &= aaaa^{-1}aaa \\ &= aaaaa \\ &= a^4 = w', \end{aligned}$$

where equality means up to reduction. Thus the free group on one generator is isomorphic to \mathbb{Z} .

The free group on two generators is much more complicated and it is not abelian. A typical reduced word might be

$$a^3b^{-2}a^5b^{13}.$$

Clearly $F_{a,b}$ has quite a few elements. Free groups have a very useful universal property.

Lemma 12.2. *Let $F = F_S$ be a free group with generators S . Let G be any group. Suppose that we are given a function $f: S \rightarrow G$.*

Then there is a unique homomorphism

$$\phi: F \rightarrow G$$

that extends f . In other words, the following diagram commutes

$$\begin{array}{ccc} S & \xrightarrow{f} & G \\ \downarrow & \nearrow \phi & \\ F & & \end{array}$$

Proof. Given a reduced word w in F , send this to the element given by replacing every letter by its image in G . It is easy to see that this is a homomorphism, as there are no relations between the elements of F . \square

In other words if $S = \{a, b\}$ and you send a to g and b to h then you have no choice but to send $w = a^2b^{-3}a$ to $g^2h^{-3}g$, whatever that element is in G .

This gives us a convenient way to present a group G . Pick generators S of G . Then we get a homomorphism

$$\phi: F_S \longrightarrow G.$$

As S generates G , ϕ is surjective. Let the kernel be H . By the First Isomorphism Theorem, G is isomorphic to F_S/H . To describe H , we need to write down generators R for H . These generators are called relations, since they describe relations amongst the generators, such that if we mod out by these relations, then we get G .

Definition 12.3. A **presentation** of a group G is a choice of generators S of G and a description of the **relations** R amongst these generators.

It is probably easiest to give some examples.

Let G be a cyclic group of order n . Pick a generator a . Then we get a homomorphism

$$\phi: F_a \longrightarrow G.$$

The kernel of ϕ is equal to H , which contains all elements of the form a^m , where m is a multiple of n , $H = \langle a^n \rangle$. Thus a presentation for G is given by the single generator a with the single relation $a^n = e$.

Take the group D_4 , the symmetries of the square. This has two natural generators g and f , where g is rotation through $\pi/2$ and f is reflection about a diagonal.

Thus we get a map

$$F_{a,b} \longrightarrow D_4$$

given by sending a to g and b to f . What are the relations, that is, what is the kernel? Well $f^2 = e$ and $g^4 = e$, so two obvious elements

of the kernel are f^2 and g^4 . On the other hand

$$fgf^{-1} = g^{-1}.$$

Using this relation, any word w can be manipulated into the form

$$f^i g^j,$$

where $i \in \{0, 1\}$ and $j \in \{0, 1, 2, 3\}$. Since this gives eight elements of the quotient and there are eight elements of G , it follows that the kernel is generated by

$$f^2, g^4, fgf^{-1}g.$$

The relations are

$$f^2 = e, g^4 = e, fgf^{-1} = g^{-1}.$$

Definition 12.4. *Let S be a set. The **free abelian group** A_S **generated by** S is the quotient of F_S , the free group generated by S , and the relations R given by the commutators of the elements of S .*

Let $S = \{a, b\}$. Then $A_{a,b}$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$. Similarly for any finite set.

Lemma 12.5. *Let S be any set and let G be any abelian group. Given any map $f: S \rightarrow G$ there is a unique homomorphism*

$$A_S \rightarrow G.$$

Proof. As F_S is a free group, there is a unique homomorphism

$$\phi: F_S \rightarrow G.$$

As G is abelian the kernel of ϕ contains the commutator subgroup. But then, as A_S is by definition the quotient of F_S by the commutator subgroup, there is a unique map $A_S \rightarrow G$ extending f . \square

Lemma 12.6. *Let G be any finitely generated abelian group.*

Then G is a quotient of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$.

Proof. Pick a finite set of generators S of G . By (12.5) there is a unique homomorphism

$$A_S \rightarrow G.$$

As S generates G this map is surjective. On the other hand A_S is isomorphic to a direct sum of copies of \mathbb{Z} . \square

Theorem 12.7. *Let G be a finitely generated abelian group.*

Then G is isomorphic to $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \times T$, where T may be presented uniquely as either,

- (1) $\mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_r}$, where each q_i is a power of a prime, or
- (2) $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$, where $m_i | m_{i+1}$.

Given this, we can classify all abelian groups of a fixed finite order. For example, take $n = 60 = 2^2 \cdot 3 \cdot 5$. Then we have

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \quad \text{or} \quad \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5,$$

using the first representation, or

$$\mathbb{Z}_2 \times \mathbb{Z}_{30} \quad \text{or} \quad \mathbb{Z}_{60}$$

using the second representation.

Finally let me mention that in general if one is given generators and relations, it can be very hard to describe the resulting quotient.

Theorem 12.8. *There is no effective algorithm to solve any of the following problems,*

Given relations R , decide if

- (1) two words w_1 and w_2 are equivalent, modulo the relations.*
- (2) a word w is equivalent, modulo the relations, to the identity.*

Succinctly, the method of representing groups by generators and relations is an art not a science.

Let's now try to classify all groups of order at most ten, up to isomorphism. To do this we recall some basic results. First note that for every natural number n , there is at least one group of order n , namely a cyclic group of order n .

Lemma 12.9. *Let G be a group of order a prime p .*

Then G is cyclic.

Proof. Pick any element g of G other than the identity and let H be the subgroup generated by g . Then the order of H is greater than one and divides the order of G , by Lagrange. As the order of G is a prime, it follows that $H = G$ so that G is cyclic, generated by any element other than the identity. \square

Look at the numbers from one to ten. Of these, 2, 3, 5 and 7 are prime. Thus by (12.9) there is exactly one group of order 1, 2, 3, 5 and 7, up to isomorphism.

The numbers that are left are 4, 6, 8, 9 and 10. The next thing to do is to start looking for interesting subgroups. The easiest way to find a subgroup, is to pick an element and look at the cyclic subgroup that it generates.

Lemma 12.10. *Let G be a group in which every element has order two.*

Then G is abelian.

Proof. Suppose that a , b and ab all have order two. We will show that a and b commute. By assumption

$$\begin{aligned} e &= (ab)^2 \\ &= abab. \end{aligned}$$

As a and b are their own inverses, multiplying on the left by a and then b , we get

$$ba = ab. \quad \square$$

On the other hand, the classification of finite abelian groups is easy. There are two of order 4,

$$\mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_4,$$

one of order six,

$$\mathbb{Z}_6,$$

three of order 8,

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_8,$$

two of order nine,

$$\mathbb{Z}_3 \times \mathbb{Z}_3, \quad \mathbb{Z}_9,$$

and one of order ten

$$\mathbb{Z}_{10}.$$

Let us start with order four. Let $g \in G$ be an element of G other than the identity. Then the order of g is 2 or 4. If it is four then G is cyclic. Otherwise g has order two. If G is not cyclic then, every element, other than the identity, must have order two, and G is abelian, by (12.10). Thus every group of order 4 is abelian.

Now suppose that G has order six. If G is abelian, then G is cyclic. Otherwise, every element of G has order two or three. By (12.10) not every element has order two. Let a be an element of order three. Let $H = \langle a \rangle$.

Lemma 12.11. *Let G be a group and let H be a subgroup of index two.*

Then H is normal in G .

Proof. It suffices to prove that the set of left cosets is equal to the set of right cosets.

The left cosets, partition the elements of G into two parts. One part is equal to H . By definition of a partition, the other part is the complement of H . By the same token, the right cosets consist of H and its complement.

Hence both partitions are equal and H is normal. \square

Pick $b \in G$, where $b \notin H$. As H has index two, G/H has order two. Thus $b^2 \in H$. If $b^2 \neq e$, then $b^2 = a$ or $b^2 = a^2$ and b has order six, a contradiction. Thus $b^2 = e$ and b has order two. Clearly $G = \langle a, b \rangle$. Consider the conjugate of a by b ,

$$bab^{-1}.$$

As H is normal in G , $bab^{-1} \in G$, so that $bab^{-1} = a$ or $bab^{-1} = a^2$. If the former then $ab = ba$ and G is abelian. Otherwise G is isomorphic to D_3 as they both have the same presentation. Thus there are two groups of order 6, a cyclic group and S_3 .

Now suppose that the order is ten. If G is not abelian, then every element, other than the identity must have order 2 or 5. Not every element has order two. Let a be an element of order five. Let $H = \langle a \rangle$. Then H has index two. Thus H is normal in G . Let $b \in G$, $b \notin H$. As before $b^2 = e$. Once again consider the conjugate of a by b ,

$$bab^{-1}$$

This is an element of H , of order five. Thus $bab^{-1} = a^i$, some $i \neq 0$. Suppose that $i \neq 1$, else G is abelian. If $i = 4$, then $bab^{-1} = a^{-1}$ and G is isomorphic to D_5 , the symmetries of a pentagon.

Suppose that $bab^{-1} = a^2$. Then

$$\begin{aligned} a &= b^2ab^{-2} \\ &= b(bab^{-1})b^{-1} \\ &= ba^2b^{-1} \\ &= (bab^{-1})(bab^{-1}) \\ &= a^2a^2 \\ &= a^4. \end{aligned}$$

But then $a^4 = a$ and so $a^3 = e$, a contradiction. Similarly $bab^{-1} \neq a^3$. Thus a group of order ten is either cyclic or isomorphic to D_5 .

Now suppose that G is a non-abelian group of order eight. There are no elements of order eight, as G is not cyclic and not every element has order two, by (12.10).

Thus G has an element a of order 4. Let $H = \langle a \rangle$. Then H has index two in G . Pick $b \in G$, with $b \notin H$. Then $b^2 \in H$. $b^2 \neq a, a^3$, otherwise b has order 8.

There are two possibilities. $b^2 = e$. In this case, consider as before, the conjugate of a by b . As before, we must have $bab^{-1} = a^3$ and we have the dihedral group D_4 . Call this group G_1 .

Otherwise $b^2 = a^2$. Call this group G_2 . Again we consider the conjugate of a by b . It must be a^3 as before. Note that this rule translates to $ba = a^3b$. Let $H = \langle a \rangle$ and $K = \langle b \rangle$. Then $G = \langle a, b \rangle = H \vee K = HK$, where we use the rule

$$ba = a^3b,$$

to prove that HK is closed under products and inverses, so that HK is a subgroup of G . We will see later that there is indeed a group of order eight with this presentation. Note that G_1 and G_2 are not isomorphic. Indeed G_1 has only two elements of order 4, a and a^3 , whilst G_2 has at least three, a , a^3 and b .

Finally consider the case where G has order nine. Then every element of G , other than the identity must have order 3. Pick an element $a = e$ and let $H = \langle a \rangle$. Let S be the set of left cosets of H in G . Then S has three elements. As in the proof of Cayley's Theorem there is a group homomorphism

$$\phi: G \longrightarrow A(S) \simeq S_3$$

We send $g \in G$ to the permutation of S that sends aH to gaH . The kernel of ϕ is a normal subgroup of G that is contained in H . The image of ϕ has order at most six, and as G has order nine, the kernel of ϕ cannot be the trivial subgroup. It follows that $\text{Ker } \phi = H$ so that H is normal in G .

Pick $b \in G - H$. Then bH is an element of G/H and so it must have order three. In particular $b^3 \in H$. But then $b^3 = e$, else b has order nine. Let $K = \langle b \rangle$. By symmetry K is normal in G . As $H \cap K = \{e\}$, it follows that the elements of H and K commute. But $G = \langle a, b \rangle$. Thus G is abelian, a contradiction.

MIT OpenCourseWare
<http://ocw.mit.edu>

18.703 Modern Algebra
Spring 2013

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.